MURRAY

Domains of Rationality and their Groups

Mathematics

A. B.

1915

DOMAINS OF RATIONALITY AND THEIR GROUPS

BY

FORREST HAMILTON MURRAY

THESIS

FOR THE

DEGREE OF BACHELOR OF ARTS

IN

MATHEMATICS

COLLEGE OF LIBERAL ARTS AND SCIENCES

UNIVERSITY OF ILLINOIS

1915

UNIVERSITY OF ILLINOIS

May 29 1915

THIS IS TO CERTIFY THAT THE THESIS PREPARED UNDER MY SUPERVISION BY

Forrest Hamilton Murray

ENTITLED Domains of Rationality and Their Groups.

IS APPROVED BY ME AS FULFILLING THIS PART OF THE REQUIREMENTS FOR THE

DEGREE OF Bachelor of Arts

G. E. Wahlin

Instructor in Charge

APPROVED: E. J. Townsend

HEAD OF DEPARTMENT OF Mathematics

CONTENTS.

DOMAINS OF RATIONALITY AND THEIR GROUPS.

CHAPTER I. DOMAINS.

An algebraic number is defined to be a number satisfying an equation of the form

$$a_0 x^n + a_1 x^{n-1} + - - - + a_{n-1}x + a_n = 0$$

of which the coefficients a_0, a_1, - - a_{n-1}, a_n are rational numbers not all zero. From this definition it can be proved that the roots of an equation with algebraic coefficients are algebraic numbers, and also that every rational function with rational coefficients of two or more algebraic numbers is an algebraic number.

If Ω is a set of numbers such that, when α, β are numbers in Ω, $\alpha+\beta$, $\alpha-\beta$, $\alpha\beta$, and $\frac{\alpha}{\beta}$ when β is not equal to zero, are also numbers in Ω, then all numbers which can be obtained from α, β by the rational processes of addition, subtraction, multiplication, and division are numbers in Ω, and Ω is defined to be a domain, or a domain of rationality. If the numbers in the domain can all be expressed as rational functions of a single number α, then the domain is denoted by $\Omega(\alpha)$.

Every domain which contains numbers not all zero must contain all rational numbers; for if $\alpha \neq 0$, $\frac{\alpha}{\alpha} = 1$, and from 1 all rational numbers can be generated by the above processes. If α is an algebraic number all numbers in $\Omega(\alpha)$ are also algebraic numbers, and $\Omega(\alpha)$ is an algebraic domain. If $\Omega(\alpha)$ contains an irrational number then $\Omega(\alpha)$ contains $\Omega(1,)$ but is not identical with $\Omega(1)$. Such a domain $\Omega(\alpha)$ which includes another domain $\Omega(\beta)$ but is not identical with it is called a domain over $\Omega(\beta)$; and $\Omega(\beta)$ is a sub-domain of $\Omega(\alpha)$.

If $\Omega(\alpha)$ is a given domain, and if β is a number not in $\Omega(\alpha)$, then if β , together with all numbers which can be derived from α and β by the processes of addition, subtraction, multiplication and division are added to $\Omega(\alpha)$, then β is said to be adjoined to $\Omega(\alpha)$. The new domain is evidently the set of all rational functions of α and β with rational coefficients, and contains $\Omega(\alpha)$ as a sub-domain. It is denoted by $\Omega(\alpha,\beta)$.

A function

$$f(x) = a_0 x^n + a_1 x^{n-1} + - - - + a_{n-1} x + a_n$$

is said to belong to a domain $\Omega(\alpha)$ if its coefficients are numbers in $\Omega(\alpha)$. A function is reducible in $\Omega(\alpha)$ if it can be broken up into factors whose coefficients are numbers in $\Omega(\alpha)$. If it cannot be broken up into factors in this way it is termed irreducible in $\Omega(\alpha)$. If a function is termed irreducible without reference to any particular domain, $\Omega(1)$, the domain of rational numbers, will be understood.

If $f(x)$ is a function irreducible in $\Omega(1)$, and if α is a root of $f(x) = 0$, then if α is also a root of $F(x) = 0$, $F(x)$ must be divisible by $f(x)$.

For $F(x)$ and $f(x)$ must have some common factor, of which α is one root; the highest common factor of $F(x)$ and $f(x)$ is obtained from these functions by rational processes, and therefore must have its coefficients in the same domain, $\Omega(1)$. It cannot be of lower degree than the degree of $f(x)$, for in that case $f(x)$ would have a rational factor. It must then be of the same degree, and is identical with $f(x)$ except for some constant factor.

Theorem I. Every rational function of α in $\Omega(1)$ can be represented as a rational integral function of α in $\Omega(1)$, of

degree not higher than n-1, where n is the degree of the irreducible equation of which α is a root.

Proof:

Let θ be any rational function of α, and suppose that

$$\theta = \frac{\phi(\alpha)}{\chi(\alpha)}.$$

Then $\chi(\alpha) \neq 0$, and consequently $\chi(x)$ and $f(x)$ are prime to each other; for otherwise $\chi(x)$ would be divisible by $f(x)$, and as a result $\chi(\alpha) = 0$.

Hence by a theorem of algebra there can be found an $F(x)$ and a $X(x)$ such that

$$F(x) \cdot f(x) + X(x)\,\chi(x) = 1.$$

Then $\qquad \phi(x)\,F(x)\,f(x) + \phi(x)X(x)\,\chi(x) = \phi(x).$

Now if $\phi(x)X(x)$ is divided by $f(x)$,

$$\phi(x)X(x) = f_1(x)\,f(x) + R(x),$$

where $R(x)$ is of lower degree than the degree of $f(x)$;

then

$$\phi(x)F(x)f(x) + \chi(x)\,\left[f_1(x)f(x) + R(x)\right] = \phi(x),$$

and if $x = \alpha$,

$$\chi(\alpha)\,R(\alpha) = \phi(\alpha).$$

$$R(\alpha) = \frac{\phi(\alpha)}{\chi(\alpha)}.$$

This representation of θ is unique; for if

$$\theta = R(\alpha) = S(\alpha),$$

where R and S are each of degree $n-1$ or less, and both are functions in (1),

$$F(x) \equiv R(x) - S(x) = 0$$

is an equation of degree less than the degree of $f(x)$, and having a root α in common with $f(x) = 0$. Since $f(x)$ is irreducible in

$\Omega(1)$, this is impossible unless all the coefficients of $F(x)$ are zero; that is,

$$R(x) \equiv S(x),$$

and the two representations are identical.

A theorem of fundamental importance is the following.

Theorem 11. Any given domain $\Omega(\alpha, \beta, --)$ can be generated by some one number in the domain.

This is equivalent to the statement that the simultaneous adjunction of any number of algebraic numbers is the same as the adjunction of some one number to a given domain.

Proof:

$$\begin{array}{llllllll} & \text{Let } \alpha \text{ be a root of the equation} & A(x) & = & 0, \\ \text{and} & \text{" } \beta \text{ " " " } \quad \text{" " } \quad \text{"} & B(x) & = & 0, \\ & - \; - \; - \; - \; - \; - \; - \; - \; - \; - \; - \; - & & & \end{array}$$

where A, B, - - are functions in $\Omega(1)$. Then suppose that

$$\alpha_1, \; \alpha_2, \; - - - \quad \alpha_m$$

represent the totality of distinct roots of these equations.

$$\begin{aligned} \text{Let} \quad \zeta_1 &= a\alpha + b\beta + c\gamma - - - , \\ \zeta_2 &= a\alpha_1 + b\alpha_2' + c\alpha_3' - - - , \\ & - - - - - - - - - - - - , \\ \zeta_p &= a\alpha_1^{(p-1)} + b\alpha_2^{(p-1)} + c\alpha_3^{(p-1)} - - - , \end{aligned}$$

where $\alpha_1^{(i)}, \alpha_2^{(i)} \cdots \alpha_j^{(i)}$ are the same as $\alpha_1, \alpha_2 \cdots \alpha_j$ in some different order, and suppose that $\zeta_1, \zeta_2, \cdots \zeta_p$ are all possible functions which can be obtained from ζ_1 by permuting the roots in all possible ways. Then a, b, c, - - can be so chosen rationally that these functions are all distinct; for if

$$F(a, b, c, -) = (\zeta_1 - \zeta_2)(\zeta_1 - \zeta_3) - - (\zeta_{p-1} - \zeta_p),$$

by a theorem of algebra a, b, c, - can be so chosen that they do

not satisfy this equation, and in an infinite varity of ways.

Let $\phi(t) = (t-\zeta_1)(t-\zeta_2) - - (t-\zeta_p)$.

Then $\phi(t)$ is a function in $\Omega(1)$, since its coefficients are rational symmetric functions of α, β, - - , and therefore are rational symmetric functions of the coefficients of the functions $A(x)$, $B(x)$, - - , which are numbers in $\Omega(1)$ by hypothesis.

Now let θ be any rational function in $\Omega(1)$ of α, β, - -, and let

$$\theta_2, \quad \theta_3, \quad - - \quad \theta_p,$$

be the functions resulting when α, β, - - are permuted in every possible way; and suppose that ζ_i, θ_i, are obtained, respectively, from ζ_1, θ_1, by the same permutation of the roots.

Then if
$$\phi(t)\left\{\frac{\theta_1}{t-\zeta_1} + \frac{\theta_2}{t-\zeta_2} + - + \frac{\theta_p}{t-\zeta_p}\right\} = F(t),$$

the coefficients of $F(t)$ are rational symmetric functions of the roots of the given equations, and are therefore rational functions of the coefficients of these equations. $F(t)$ is therefore a function in $\Omega(1)$.

Hence
$$F(\zeta_1) = \theta_1\phi'(\zeta_1),$$
$$\theta_1 = \frac{F(\zeta_1)}{\phi'(\zeta_1)}.$$

It follows from this theorem that the discussion of any given domain $\Omega(\alpha, \beta, - -)$ can be replaced by the discussion of a domain generated by a single number, $\Omega(\zeta)$. The domains considered here are algebraic domains, or domains generated by algebraic numbers; this theorem would not necessarily hold for domains other than algebraic domains,. according to this method of proof.

CHAPTER II. SUBSTITUTIONS OF A DOMAIN.

Given a domain $\Omega(\alpha)$, suppose that each number ω in $\Omega(\alpha)$ is replaced by some number ω', in such a way that $\omega_1+\omega_2$ is replaced by $\omega_1'+\omega_2'$, $\omega_1-\omega_2$ by $\omega_1'-\omega_2'$, $\omega_1\omega_2$ by $\omega_1'\omega_2'$, $\frac{\omega_1}{\omega_2}$ by $\frac{\omega_1'}{\omega_2'}$; then such a substitution is called a substitution of the domain $\Omega(\alpha)$, providing the correspondence thus established is a one-to-one correspondence.

The domain $\Omega(\alpha)$ has been defined as the domain generated by α; such a number α, in terms of which every number in the domain can be expressed, is defined to be a primitive number of the given domain.

Theorem I. If α_1 is a primitive number in a domain $\Omega(\beta)$, and if α_2, α_3, - - α_n, are the other roots of the irreducible equation in $\Omega(1)$ of which α_1 is a root, then all substitutions of the form (α_1, γ) are substitutions of the domain when and only when γ is one of the roots α_1, α_2, - - α_n.

Proof:

Suppose every number in the domain $\Omega(\alpha)$ represented as some function of α with rational coefficients. 0 and 1 will have a possible representation as $\alpha_1-\alpha_1$, $\frac{\alpha_1}{\alpha_1}$, respectively.

Then if α' represents the number corresponding to α,

$$(\alpha-\alpha)' = \alpha'-\alpha',$$

hence $0' = 0$;

Also, $\left(\frac{\alpha}{\alpha}\right)' = \frac{\alpha'}{\alpha'}$

and therefore $1' = 1$.

From this it follows that if α' corresponds to α in any substitution of the domain, every rational number corresponds to

itself in every substitution of the domain.

Now if α is a primitive number in $\Omega(\beta)$, let any number θ_1 in $\Omega(\beta)$ be represented

$$\begin{aligned}\theta_1 &= \phi_1(\alpha)\\ &= a_1\alpha^{n-1} + a_2\alpha^{n-2} + \cdots + a_{n-1}\alpha + a_n.\end{aligned}$$

This representation has been shown to be unique.

Then let

$$\begin{aligned}\theta_2 &= \phi_2(\alpha)\\ &= b_1\alpha^{n-1} + b_2\alpha^{n-2} + \cdots + b_{n-1}\alpha + b_n,\end{aligned}$$

where $\theta_2 \neq \theta_1$.

Then if α is replaced by α', another root of the irreducible equation $f(x) = 0$,

let
$$\theta_1' = \phi_1(\alpha'),$$
$$\theta_2' = \phi_2(\alpha').$$

Now if $\theta_2' = \theta_1'$,

$$\phi_1(\alpha') = \phi_2(\alpha'),$$

and $F(\alpha') \equiv \phi_1(\alpha') - \phi_2(\alpha') = 0$

is an equation in $\Omega(1)$ of degree n-1 or less, of which α' is a root. Then F(x) must vanish identically, since if it possessed a degree f(x) would be reducible in $\Omega(1)$, contrary to hypothesis.

But if $\phi_1(x) \equiv \phi_2(x)$,

$$\phi_1(\alpha) = \phi_2(\alpha),$$

and $\theta_2 = \theta_1$,

contrary to hypothesis. Therefore the correspondence thus established is a one-to-one correspondence.

Also, if

$$\theta_1 + \theta_2 = \phi_1(\alpha) + \phi_2(\alpha) = F(\alpha),$$
$$(\theta_1 + \theta_2)' = \phi_1(\alpha') + \phi_2(\alpha') = F(\alpha'),$$

and by the substitution of α' for α in $F(\alpha)$, $\theta_1'+\theta_2'$ corresponds to $\theta_1+\theta_2$.

Similarly, if

$$\begin{aligned} (\theta_1 \theta_2) &= \phi_1(\alpha)\, \phi_2(\alpha) = F_2(\alpha), \\ (\theta_1 \theta_2)' &= F_2(\alpha') = \phi_1(\alpha')\, \phi_2(\alpha') \\ &= \theta_1'\, \theta_2'; \end{aligned}$$

if

$$\begin{aligned} (\theta_1-\theta_2) &= \phi_1(\alpha) - \phi_2(\alpha) = F_3(\alpha), \\ (\theta_1-\theta_2)' &= F_3(\alpha') = \phi_1(\alpha') - \phi_2(\alpha') \\ &= \theta_1'-\theta_2', \end{aligned}$$

and if

$$\begin{aligned} \frac{\theta_1}{\theta_2} &= \frac{\phi_1(\alpha)}{\phi_2(\alpha)} = F_4(\alpha), \\ \left(\frac{\theta_1}{\theta_2}\right)' &= F_4(\alpha') = \frac{\phi_1(\alpha')}{\phi_2(\alpha')} \\ &= \frac{\theta_1'}{\theta_2'}, \end{aligned}$$

and the substitution (α,α') is a substitution of the domain.

Now if β is not a root of the irreducible equation in $\Omega(1)$ of which α is a root, then, conversely, α is not a root of the irreducible equation of which β is a root.

Let $B(x)$ be the irreducible equation of which β is a root, and therefore

$$\begin{aligned} B(\beta) &= 0, \\ B(\alpha) &\neq 0 \\ &= \gamma\text{, say.} \end{aligned}$$

Then, since

$$\begin{aligned} \alpha - \alpha &= 0, \\ \beta - \beta &= 0, \end{aligned}$$

by means of the substitution (α,β) two distinct numbers, γ and 0 are made to correspond to one number 0. This correspondence is not a one-to-one correspondence, and consequently the substitution (α,β) is not a substitution of the domain.

Given a domain $\Omega(\alpha)$, then if β is some number in the domain, the numbers β_1, β_2, - - β_m which can be made to correspond to β by

means of substitutions of the domain are said to be conjugate to β_1.

Theorem II. Every number θ in $\Omega(\alpha)$ is a root of an equation of the same degree as that of the irreducible equation which α satisfies, and whose other roots are the numbers conjugate to θ.

Proof:

Let $\theta_1 = \phi(\alpha_1)$, $\theta_2 = \phi(\alpha_2)$, - - $\theta_n = \phi(\alpha_n)$,

and form the function

$$\Phi(t) = (t - \theta_1)(t - \theta_2) \;--\; (t - \theta_n).$$

Now the coefficients of $\Phi(t)$ are symmetric functions of the numbers θ_1, θ_2, - - θ_n, hence of the roots α_1, α_2, - - α_n, and consequently may be expressed rationally in terms of the coefficients of the equation which α satisfies. $\Phi(t)$ is therefore a function in $\Omega(1)$.

$\Phi(t)$ is either irreducible or a power of an irreducible function; for if

$$\Phi(t) = \phi_1(t)\,\phi_2(t),$$

$\phi_1(t)$ vanishes for some one of the conjugates θ_i, say.

$$\phi_1(\theta_i) = 0.$$

That is, $\phi_1[\phi(\alpha_i)] = 0$,

or $F(\alpha_i) = 0$.

Then $F(x)$ must be divisible by $f(x)$, the function irreducible in $\Omega(1)$ which vanishes for $x = \alpha$.

Hence

$$F(\alpha_1) = F(\alpha_2) = \;---\; F(\alpha_n) = 0.$$

But $F(\alpha_1) = \phi_1(\theta_1)$, $F(\alpha_2) = \phi_1(\theta_2)$, - - -

therefore $\phi_1(t)$ vanishes for all roots of $\Phi(t) = 0$, and every rational factor has this same property. This can only be possible when $\Phi(t)$ is some power of $\phi_1(t)$.

Then $\Phi(t) = [\phi(t)]^m$, and if $\underline{r}$ is the degree of $\phi(t)$, $n = mr$.

Theorem III. A necessary and sufficient condition that a number α be primitive in a domain $\Omega(\beta)$ is that α be distinct from all its conjugates.

A. Assume α primitive in $\Omega(\beta)$.

Let $\alpha = \phi(\beta)$.

Then $\beta = F(\alpha)$,

where F is the inverse function of ϕ.

Let
$$\beta' = F(\alpha'),$$
$$\beta'' = F(\alpha''),$$
$$- - - - - -$$
$$\beta^{(n-1)} = F(\alpha^{(n-1)}).$$

Then $(t-\beta)(t-\beta') - - \quad (t-\beta^{(n-1)}) = \Phi(t)$

is a function in $\Omega(1)$, since its coefficients are rational symmetric functions of the β's. Hence if $\underline{m}$ is the degree of the irreducible equation of which β is a root, by the preceding theorem $m \leq n$.

Also,
$$\alpha = \phi(\beta),$$
$$\alpha' = \phi(\beta'),$$
$$- - - - - -$$
$$\alpha^{(m-1)} = \phi(\beta^{(m-1)}).$$

Then $(t-\alpha)(t-\alpha') - - \quad (t-\alpha^{(m-1)}) = \chi(t)$

is again a function in $\Omega(1)$, which vanishes for $t=\alpha$; it must therefore be of degree at least as great as $\underline{n}$. Then $m \geq n$, and by combining these two results we obtain

$$m = n.$$

Therefore α has the same number of conjugates as β, and these must then be distinct; for if two or more conjugates were

equal, by the preceding theorem $\chi(t)$ would be a power of an irreoucible function, and would necessarily be reducible. $\chi(t)$, however, is of the same degree as that of an irreducible function which has a root α in common with it, and this is impossible.

B. Assume α distinct from all its conjugates.

Let ω be any number in $\Omega(\beta)$, ω', ω'', - - $\omega^{(n-1)}$, its conjugates.

Now if
$$\Phi(t) = (t-\alpha)(t-\alpha') \; - \; - \; (t-\alpha^{(n-1)}),$$

$\Phi(t)$ is necessarily irreducible, by the preceding theorem, and hence can have no multiple roots.

$$\text{Let} \quad \Phi(t)\left\{\frac{\omega}{t-\alpha} + \frac{\omega'}{t-\alpha'} + - - + \frac{\omega^{(n-1)}}{t-\alpha^{n-1}}\right\} = \Psi(t).$$

Then $\Psi(t)$ is a function in $\Omega(1)$, since its coefficients are rational symmetric functions of the α's.

$$\Phi'(\alpha)\,\omega = \Psi(\alpha),$$

$$\omega = \frac{\Psi(\alpha)}{\Phi'(\alpha)},$$

and ω is expressed rationally in terms of α.

By the above theorem every primitive number in the domain $\Omega(\beta)$ is a root of an irreducible equation in $\Omega(1)$ of degree n, for if it is distinct from all its conjugates these cannot be less than n-1 in number, while an equation in $\Omega(1)$ of degree n can be formed having the given primitive number as a root. The number n is therefore characteristic of the domain $\Omega(\beta)$, and is defined to be the order of the domain.

Then if ω is any number in $\Omega(\alpha)$, the order of $\Omega(\omega)$ is a factor of the order of $\Omega(\alpha)$. For if ω has k-1 distinct conjugates, ω is a root of an irreducible equation in $\Omega(1)$ of degree k. k is a factor of n, by Theorem II, and since k is the order of

$\Omega(\omega)$ the truth of the statement follows.

If a domain $\Omega(\alpha)$ contains no sub-domain except $\Omega(1)$ it is defined to be a *primitive* domain. Every domain of prime order is evidently primitive, since if it contained a sub-domain its order would be divisible by the order of this sub-domain, which is impossible.

If $\alpha', \alpha'', - - \alpha^{(n-1)}$, are the conjugates of α, $\Omega(\alpha)$, $\Omega(\alpha')$, - - - - $\Omega(\alpha^{(n-1)})$ are called *conjugate* domains. A domain which is identical with all its conjugate domains is called a *normal* or *Galois* domain. An equation is defined to be a normal or Galois equation if it is irreducible and has the property that every one of its roots can be expressed rationally in terms of some one of them.

If $F(x) = 0$ is an equation in $\Omega(1)$ having no multiple roots, the domain $\Omega(\alpha_1, \alpha_2, - - \alpha_m)$ obtained by adjoining to $\Omega(1)$ all roots of $F(x) = 0$ is a Galois domain according to the above definition.

For if ζ is a primitive number in $\Omega(\alpha_1, \alpha_2 - - \alpha_m)$,

$$\zeta = f(\alpha_1, \alpha_2, - - \alpha_m).$$

Then if

$$\zeta' = f(\alpha_1', \alpha_2', - - \alpha_m'),$$

$$- - - - - - - - - - - -$$

$$\zeta^{(n-1)} = f(\alpha_1^{(n-1)}, \alpha_2^{(n-1)}, - - \alpha_m^{(n-1)}),$$

where $\alpha_1^{(i)}, \alpha_2^{(i)}, - - \alpha_m^{(i)}$, are the same as $\alpha_1, \alpha_2, - - \alpha_m$ in some different order, $\zeta', \zeta'', - - \zeta^{(n-1)}$, are also in the given domain, and by definition the domain is a Galois domain.

An equation $g(t) = 0$ is a Galois *resolvent* of a given equation $F(x) = 0$, whose coefficients are rational numbers, if (1), $g(t)$ is irreducible, (2), every root of $F(x) = 0$ can be expressed rationally in terms of a root ρ of $g(t) = 0$, and (3),

a root ρ of $g(t)$ can be expressed rationally in terms of the roots of the equation $F(x) = 0$.

Theorem 1V. Given $\Omega(\rho)$ a normal domain of order $\underline{m}$, and $\rho_2, \rho_3, -- \rho_m$, the conjugates of ρ; then by the substitution (ρ,ρ_a) the ρ s are merely interchanged among themselves.

For, let

$$\rho_2 = \theta_2(\rho), \quad \rho_3 = \theta_3(\rho), \quad -- \quad \rho_m = \theta_m(\rho).$$

Then by the substitution (ρ,ρ_i) ρ_j goes over into $\theta_j(\rho_i)$.

Now

$$g(\rho_j) = g\left[\theta_j(\rho)\right] = F(\rho) = 0.$$

Therefore $F(x)$ is divisible by $g(x)$, and

$$F(\rho) = F(\rho_2) = -- \quad F(\rho_m) = 0.$$

But $$F(\rho_i) = g\left[\theta_j(\rho_i)\right],$$

and hence $$\theta_j(\rho_i) = \rho_k,$$

some one of the roots $\rho, \rho_2, -- \rho_m$ This proves the theorem.

Theorem V. Every substitution (ρ,ρ_a) can be represented in the form (ρ_h, ρ_k), where either ρ_h or ρ_k is given, and the other is then uniquely determined by (ρ,ρ_a).

Proof:

Let $$\rho_2 = \theta_2(\rho), \quad \rho_3 = \theta_3(\rho), \quad -- \quad \rho_m = \theta_m(\rho).$$

Then if

$$\omega = f(\rho_h),$$

suppose (ρ,ρ_a) transforms ω into ω', and ρ_h into ρ_k, say.

Now

$$\omega = f\left[\theta_h(\rho)\right],$$
$$\omega' = f\left[\theta_h(\rho_a)\right];$$

then since $$\theta_h(\rho_a) = \rho_k,$$
$$\omega' = f(\rho_k).$$

Therefore (ρ_h, ρ_k) produces the same effect as (ρ,ρ_a), and the

two are identical, considered as substitutions of the domain.

Also, if ρ_k is given first, then, since ρ_a is primitive,

$$\rho_k = \phi_k(\rho_a).$$

Now $$(\rho_a, \rho) = (\rho, \rho_b)$$

for some ρ_b. Then if $F(x).\pi$ denotes the result of operating on $F(x)$ by π,

$$\phi_k(\rho_a).(\rho_a, \rho) = \phi_k(\rho).$$

By the preceding developments (ρ_a, ρ) transforms ρ_k into ρ_l, say. Then $$\rho_l = \phi_k(\rho).$$

But
$$\begin{aligned}\phi_k(\rho).(\rho, \rho_a) &= \phi_k(\rho_a).(\rho_a, \rho)(\rho, \rho_a)\\ &= \phi_k(\rho_a).\end{aligned}$$

Then since $\phi_k(\rho_a) = \rho_k$, the substitution (ρ, ρ_a) transforms ρ_l into ρ_k, and since ρ_k was the given root of the equation $g(t) = 0$, the theorem follows.

Now since $\rho_1, \rho_2, - - \rho_m$, are primitive numbers in the given domain, and roots of the same irreducible equation in $\Omega(1)$, it follows that the substitutions (ρ_1, ρ_2), (ρ_1, ρ_3), - - (ρ_1, ρ_m) are the substitutions of the given normal domain.

Theorem VI. The substitutions of a normal domain have the characteristic properties of a group.

Proof:

Let
$$\begin{aligned}(\rho, \rho_a) &= \sigma_a,\\ (\rho, \rho_b) &= \sigma_b.\end{aligned}$$

Then $$(\rho, \rho_b) = (\rho_a, \rho_c),$$

and
$$\begin{aligned}(\rho, \rho_a)(\rho, \rho_b) &= (\rho, \rho_a)(\rho_a, \rho_c)\\ &= (\rho, \rho_c),\end{aligned}$$

another substitution of the domain.

Also, if
$$\begin{aligned}\sigma_a &= (\rho, \rho_a),\\ \sigma'_a &= (\rho_a, \rho),\end{aligned}$$

then $\sigma_a\sigma_a' = (\rho,\rho)$, and every number in the domain $\Omega(\rho)$ is replaced by itself; hence $\sigma_a\sigma_a' = E$, the identical substitution, $\sigma_a' = \sigma_a^{-1}$, and every substitution of the domain has an inverse.

The associative law holds; for if

$$\sigma_a = (\rho,\rho_a),$$

$$\sigma_b = (\rho,\rho_b) = (\rho_a,\rho_k)$$

for some ρ_k, $\quad \sigma_c = (\rho,\rho_c) = (\rho_k,\rho_l)$

for some ρ_l, then

$$\begin{aligned}\sigma_a(\sigma_b\sigma_c) &= (\rho,\rho_a)[(\rho_a,\rho_k)(\rho_k,\rho_l)]\\ &= (\rho,\rho_a)(\rho_a,\rho_l)\\ &= (\rho,\rho_l).\end{aligned}$$

Also,

$$\begin{aligned}(\sigma_a\sigma_b)\sigma_c &= [(\rho,\rho_a)(\rho_a,\rho_k)](\rho_k,\rho_l)\\ &= (\rho,\rho_k)(\rho_k,\rho_l)\\ &= (\rho,\rho_l).\end{aligned}$$

Therefore

$$(\sigma_a\sigma_b)\sigma_c = \sigma_a(\sigma_b\sigma_c).$$

Consequently the substitutions (ρ,ρ_a) have the characteristic properties of a group; this group is called the Galois group of the domain $\Omega(\rho)$.

Theorem VII. The Galois group is simply isomorphic with a permutation group on the roots $\alpha_1, \alpha_2, - - \alpha_n$, of the equation $F(x)=0$.

Proof:

Let $\alpha_1 = f_1(\rho)$, $\alpha_2 = f_2(\rho)$, ---- $\alpha_n = f_n(\rho)$.

When operated on by the substitution (ρ,ρ_a) these become

$$\alpha_1' = f_1(\rho_a),\quad \alpha_2' = f_2(\rho_a),\quad ----\quad \alpha_n' = f_n(\rho_a).$$

Now $\alpha_1', \alpha_2', - - \alpha_n'$, are the original roots in some different order, since every root of a given equation is transformed by (ρ,ρ_a) into some other root of the same equation, when this equation has its coefficients in $\Omega(1)$.

Consequently (ρ,ρ_a) gives rise to a certain permutation of the

α's,

$$\begin{pmatrix}\alpha_1, \alpha_2, \alpha_3, & - & - \alpha_n \\ \alpha_1', \alpha_2', \alpha_3', & - & - \alpha_n'\end{pmatrix}.$$

Also, the permutation

$$\begin{pmatrix}\alpha_1, \alpha_2, \alpha_3 & - & - \alpha_n \\ \alpha_1', \alpha_2', \alpha_3' & - & - \alpha_n'\end{pmatrix}$$

gives rise to the substitution (ρ, ρ_a).

For if $$\begin{aligned}\rho &= \phi(\alpha_1, \alpha_2, \alpha_3 - - \alpha_n) \\ &= \phi\left[f_1(\rho), f_2(\rho), - - f_n(\rho)\right],\end{aligned}$$

this is an equation in $\Omega(1)$ which ρ satisfies, and which must therefore hold for all the roots of the Galois resolvent.

Then $$\rho_a = \phi\left[f_1(\rho_a), f_2(\rho_a), - - f_n(\rho_a)\right].$$

Therefore $$\rho_a = \phi(\alpha_1', \alpha_2', \alpha_3' - - \alpha_n').$$

Now let $$\rho_b = \phi(\alpha_1'', \alpha_2'', \alpha_3'' - - \alpha_n''),$$

and let ρ_c be so chosen that $(\rho, \rho_b) = (\rho_a, \rho_c)$. Let $\rho_c = \phi(\alpha_1''', \alpha_2'' - - \alpha_n''')$.

Then suppose that $$(\rho, \rho_a) \sim \begin{pmatrix}\alpha_1, \alpha_2, \alpha_3, & - & - \alpha_n \\ \alpha_1', \alpha_2', \alpha_3', & - & - \alpha_n'\end{pmatrix}$$

$$(\rho, \rho_b) \sim \begin{pmatrix}\alpha_1, \alpha_2, \alpha_3, & - & - \alpha_n \\ \alpha_1'', \alpha_2'', \alpha_3'', & - & - \alpha_n''\end{pmatrix}$$

$$(\rho, \rho_c) \sim \begin{pmatrix}\alpha_1, \alpha_2, \alpha_3, & - & - \alpha_n \\ \alpha_1''', \alpha_2''', \alpha_3'' & - & - \alpha_n'''\end{pmatrix}$$

Then $$(\rho_a, \rho_c) \sim \begin{pmatrix}\alpha_1', \alpha_2', \alpha_3', & - & - \alpha_n' \\ \alpha_1''', \alpha_2''', \alpha_3''' & - & - \alpha_n'''\end{pmatrix}$$

Therefore $$\begin{aligned}(\rho, \rho_a)(\rho, \rho_b) &= (\rho, \rho_a)(\rho_a, \rho_c) \\ &= (\varphi, \rho_c).\end{aligned}$$

Also, $$\begin{pmatrix}\alpha_1, \alpha_2, \alpha_3, & - & - \alpha_n \\ \alpha_1', \alpha_2', \alpha_3', & - & - \alpha_n'\end{pmatrix}\begin{pmatrix}\alpha_1, \alpha_2, \alpha_3, & - & - \alpha_n \\ \alpha_1'', \alpha_2'', \alpha_3'', & - & - \alpha_n''\end{pmatrix}$$

$$= \begin{pmatrix}\alpha_1, \alpha_2, \alpha_3, & - & - \alpha_n \\ \alpha_1', \alpha_2', \alpha_3', & - & - \alpha_n'\end{pmatrix}\begin{pmatrix}\alpha_1', \alpha_2', \alpha_3', & - & - \alpha_n' \\ \alpha_1''', \alpha_2''', \alpha_3''', & - & - \alpha_n'''\end{pmatrix} = \begin{pmatrix}\alpha_1, \alpha_2, \alpha_3, & - & - \alpha_n \\ \alpha_1''', \alpha_2''', \alpha_3''', & - & - \alpha_n'''\end{pmatrix}$$

and the correspondence is a simple isomorphism. From the fact that this correspondence can be established it follows that these permutations form a group.

The term <u>Galois group</u> will be used to denote either the group of substitutions or the group of permutations, as is most convenient in any particular discussion.

A function of the roots $\alpha_1, \alpha_2,$ - - α_n, of the equation $F(x)=0$ is said to <u>permit</u> the permutation π if it remains unchanged after the permutation π.

Theorem VIII. Every rational equation in $\Omega(1)$ which subsists between the roots of the equation $F(x) = 0$, remains valid when the roots are subjected to every permutation of the Galois group; and every rational function in $\Omega(1)$ which permits the permutations of the entire Galois group is a number in $\Omega(1)$.

For every equation between the α's can be represented as an equation in ρ; then if $\phi(\rho) = 0$,

$$\phi(\rho) = \phi(\rho_2) = \phi(\rho_3) = - - = \phi(\rho_m) = 0,$$

since $\phi(x)$ has a root in common with $g(x)$, and hence must be divisible by $g(x)$. The substitutions (ρ, ρ_i) are the same the permutations of the Galois group, and are generated by them; this proves the first part of the theorem.

Now if ω is a number in $\Omega(f)$ which is identical with all its conjugates,

$$\omega = f(\rho) = f(\rho_2) = - - = f(\rho_m),$$

by Theorem II ω is a root of an equation in $\Omega(1)$ of the first degree, and must therefore be a number in $\Omega(1)$.

Theorem IX. Every permutation of the roots of the equation $F(x) = 0$ which leaves valid all rational equations in $\Omega(1)$ subsisting between these roots is a permutation of the Galois group.

Proof:

Every such permutation π can be represented as a substitution of the form (ρ, τ), where τ is some other number in

$\Omega(\rho)$. Now $g(\rho) = 0$ can be represented as an equation between the roots of the equation $F(x) = 0$; if π leaves this equation valid,

$$g(\tau) = 0,$$

and since $g(x)$ is irreducible in $\Omega(1)$, τ must be one of the roots $\rho_1, \rho_2, - - \rho_m$, say ρ_K. Then $\pi = (\rho, \rho_K)$, and π is a substitution or permutation of the Galois group.

Theorem X. If P is a group such that it leaves valid all rational equations in $\Omega(1)$ between the roots of the equation $F(x)=0$, and such that every rational function of the roots which remains unchanged under all the permutations of P is a number in $\Omega(1)$, then P is the Galois group of the equation $F(x) = 0$.

Proof:

Let P be $\pi_1, \pi_2, - - \pi_\mu$.

Then any rational equation between the α's can be represented as an equation in ρ: $\phi(\alpha_1, \alpha_2, - - \alpha_n) = f(\rho)$.

Let the permutations of P transform ρ into

$$\rho, \rho_2, \rho_3, - - \rho_\mu,$$

and let $(t - \rho)(t - \rho) - - (t - \rho_\mu) = \omega$,

where t is some rational number. By hypothesis ω is a rational number, since it is left unchanged under all the permutations of P. ρ is, then, a root of an equation of degree μ in $\Omega(1)$; therefore all the roots of the resolvent $g(t)$ are included among the above numbers, $\mu = m$, and P, which by the preceding theorem is included in the Galois group, must be identical with it, since it is of the same order.

Theorem XI. The Galois group of a reducible equation is intransitive. If the Galois group of an equation is intransitive, every transitive system determines a rational facter of the given

function $F(x)$.

Proof:

Let $$F(x) = f_1(x)\, f_2(x), \cdots f_k(x),$$

where $f_1(x)$, $f_2(x)$, $f_k(x)$, are irreducible in $\Omega(1)$.

Then, for some α, $$f_1(\alpha) = 0.$$ $$f_2(\alpha) \neq 0,$$

since if both are irreducible in $\Omega(1)$, they can have no factor in common. Let $f_2(\beta) = 0$. Then since every permutation of the Galois group transforms rational numbers into themselves, no permutation of the group can replace β by α.

Let $\alpha_1, \alpha_2, \alpha_3, - - \alpha_{m_1},$ satisfy $f_1(x) = 0,$

$\beta_1, \beta_2, \beta_3, - - \beta_{m_2},$ " $f_2(x) = 0,$

- - - - - - - - - - - - -

$\sigma_1, \sigma_2, \sigma_3, - - \sigma_{m_k},$ " $f_k(x) = 0.$

Then no permutation of the group can replace any root in one system by any one of another system; the roots in any given system are conjugate, being roots of the same irreducible equation, and therefore the Galois group has these systems of intransitivity.

Now suppose that the above systems are the systems of intransitivity of the Galois group.

Let
$$\phi_1(t) = (t-\alpha_1)(t-\alpha_2) - - (t-\alpha_{m_1}),$$
$$\phi_2(t) = (t-\beta_1)(t-\beta_2) - - (t-\beta_{m_2}),$$
- - - - - - - - - - - -
$$\phi_k(t) = (t-\sigma_1)(t-\sigma_2) - - (t-\sigma_{m_k}).$$

Now every coefficient of $\phi_1(t)$ is a rational symmetric function of the α's; the α's are interchanged among themselves by every permutation of the Galois group, and by Theorem VIII these coefficients must be numbers in $\Omega(1)$, since they are left unchanged

by every permutation of the Galois group. Similarly, $\phi_2(t)$, $\phi_3(t)$, - - $\phi_k(t)$ are functions in $\Omega(1)$, and

$$F(t) \equiv \phi_1(t)\,\phi_2(t) \;-\;-\; \phi_k(t)$$

has these as factors in $\Omega(1)$.

Theorem XII. The Galois group of an imprimitive domain is an imprimitive group.

Proof:

Let $\rho_1, \rho_2,$ - - ρ_n, be the roots of the Galois resolvent $g(t) = 0$. Then if the Galois domain is imprimitive, there exists a number $\theta = \phi(\rho)$ having more than one and fewer than n conjugates, if n is the degree of $g(t)$.

Let

$$\theta = \phi(\rho_1) = \phi(\rho_2) = \phi(\rho_3) = - - = \phi(\rho_r),$$

these being all the functions $\phi(\rho)$ equal to θ.

Also, suppose that

$$\theta . (\rho, \rho_k) = \theta' \neq \theta .$$

$$\theta' = \phi(\rho_k) = \phi(\rho_{k+1}) = \phi(\rho_{k+2}) = - - = \phi(\rho_{k+s}).$$

Then no ρ_{k+i} in the second set can be in the first set also; for in that case $\theta = \theta'$, and there would be more than r functions equal to θ.

Also, s = r; for otherwise (ρ_k, ρ), which would transform θ' into θ, would make more than r functions $\phi(\rho)$ equal to θ.

By continuing this process one finds that

$$\begin{aligned} \theta &= \phi(\rho_1) = \phi(\rho_2) - - - = \phi(\rho_r), \\ \theta' &= \phi(\rho_{r+1}) = \phi(\rho_{r+2}) - - - = \phi(\rho_{2r}), \\ & - - - - - - - - - - - - \\ \theta^{(k-1)} &= \phi(\rho_{(k-1)r+1}) = \phi(\rho_{(k-1)r+2}) - - - = \phi(\rho_n), \end{aligned}$$

and kr = n. Every substitution of the Galois group either replaces all the roots of one set by others of the same set, or

replaces those of one set by those of some other set. The Galois group is therefore imprimitive on these systems.

Theorem XIII. If the Galois group of a domain is imprimitive the domain itself is imprimitive.

Proof:

Let $F(x) = 0$ be the given equation, irreducible in $\Omega(1)$, and let the given systems of imprimitivity be,

$$\begin{array}{l} \alpha_1,\ \alpha_2,\ \alpha_3,\ --\ \alpha_n, \\ \beta_1,\ \beta_2,\ \beta_3,\ --\ \beta_n, \\ -\ -\ -\ -\ -\ - \\ \gamma_1,\ \gamma_2,\ \gamma_3,\ --\ \gamma_n. \end{array}$$

Let
$$\begin{aligned} \omega_1 &= (t-\alpha_1)(t-\alpha_2)\ --\ (t-\alpha_n), \\ \omega_2 &= (t-\beta_1)(t-\beta_2)\ --\ (t-\beta_n), \\ &-\ -\ -\ -\ -\ -\ -\ -\ -\ - \\ \omega_k &= (t-\gamma_1)(t-\gamma_2)\ --\ (t-\gamma_n), \end{aligned}$$

where <u>t</u> is some rational number.

Then form the function

$$\phi(u) = (u-\omega_1)(u-\omega_2)\ --\ (u-\omega_k).$$

$\phi(u)$ has for its coefficients rational symmetrical functions of the ω's, and is therefore a function in $\Omega(1)$; it is irreducible in $\Omega(1)$, since any rational factor would vanish for some root ω_i, and therefore for all such roots, since these roots are conjugate under the Galois group.

Now if ζ is any rational symmetric function of $\alpha_1, \alpha_2,\ --\ \alpha_n$, ζ' the corresponding function of $\beta_1, \beta_2,\ --\ \beta_n$, and so on, then

$$\phi(u)\left\{\frac{\zeta}{u-\omega_1} + \frac{\zeta'}{u-\omega_2} + --\ + \frac{\zeta^{(k-1)}}{u-\omega_k}\right\} = \Phi(u)$$

has as coefficients rational symmetric functions of the roots of the equation $F(x) = 0$, and is therefore a function in $\Omega(1)$.

Then
$$\phi'(\omega_1)\,\zeta = \Phi(\omega_1),$$
$$\zeta = \frac{\Phi(\omega_1)}{\phi'(\omega_1)}.$$

From this result it follows that
$$\omega_1 = \Psi(t, \alpha) = \Psi_1(t, \omega_1),$$
since the α's enter as rational symmetric functions, which can therefore be expressed in terms of ω_1.

$$\Psi_1(\alpha_1,\omega_1) \equiv \alpha_1^n + f_1(\omega_1)\alpha_1^{n-1} + - - + f_n(\omega_1) = 0.$$

Or, $\Psi_1(\alpha_1,\omega_1) \equiv \omega_1^k + \phi_1(\alpha_1)\,\omega_1^{k-1} + - - + \phi_k(\alpha_1) = 0.$

Then $\Psi_1(\alpha_1,u) \equiv u^k + \phi_1(\alpha_1)u^{k-1} + - - - + \phi_k(\alpha_1) = 0.$

Now $\phi(u)$ and $\Psi_1(\alpha_1,u)$ are both satisfied by $u = \omega_1$, while $u = \omega_2$ does not satisfy $\Psi_1(\alpha_1,u) = 0$. Therefore the two functions have in common the factor $u - \omega_1$ and no other.

Then $$F(u)\,\phi(u) + G(u)\Psi_1(\alpha_1,u) = u - \omega_1.$$

Each of these component functions can have only a finite number of roots when equated to zero, and consequently a <u>k</u> can be chosen rationally in an infinite number of ways so that it does not make any of these functions vanish.

Then
$$F(k)\,\phi(k) + G(k)\Psi_1(\alpha_1,k) = k - \omega_1.$$

Hence ω_1 can be expressed rationally in terms of α_1, and the same is true of $\alpha_2, \alpha_3, - - \alpha_n$.

$$\omega_1 = \chi(\alpha_1) = \chi(\alpha_2) = - - - = \chi(\alpha_n).$$

Likewise, $\omega_2 = \chi(\beta_1) = \chi(\beta_2) = - - - = \chi(\beta_n),$

- - - - - - - - - - - - - -

$$\omega_k = \chi(\gamma_1) = \chi(\gamma_2) = - - - = \chi(\gamma_n).$$

From these equations the theorem follows.

Theorem XIV. An imprimitive domain $\Omega(\alpha)$ of the n'th order

is reduced to a domain of the r'th order over $\Omega' = \Omega(\theta)$ by the adjunction of θ to the domain $\Omega(1)$.

Proof:

Let $\Psi(x_1, x_2, - - x_n)$ be any rational symmetric function of the x's, and let

$$\omega_1 = \Psi(\alpha_1, \alpha_2, - - \alpha_n),$$
$$\omega_2 = \Psi(\beta_1, \beta_2, - - \beta_n),$$
$$- - - - - - - - -$$
$$\omega_k = \Psi(\gamma_1, \gamma_2, - - \gamma_n),$$

where these sets are the systems of imprimitivity of the domain.

Also, let θ_1 be any other function such that

$$\theta_1 = \chi(\alpha_1) = \chi(\alpha_2) = - - = \chi(\alpha_n),$$
$$\theta_2 = \chi(\beta_1) = \chi(\beta_2) = - - = \chi(\beta_n),$$
$$- - - - - - - - - - - - -$$
$$\theta_k = \chi(\gamma_1) = \chi(\gamma_2) = - - = \chi(\gamma_n).$$

Let $\phi(u) = (u-\theta_1)(u-\theta_2) - - (u-\theta_k).$

Then $\phi(u)$ is a function in $\Omega(1)$, and likewise

$$\phi(u)\left\{\frac{\omega_1}{u-\theta_1} + \frac{\omega_2}{u-\theta_2} + - - - + \frac{\omega_k}{u-\theta_k}\right\} = \Phi(u)$$

is a function in $\Omega(1)$.

Then $$\omega_1\,\phi'(\theta_1) = \Phi(\theta_1),$$
$$\omega_1 = \frac{\Phi(\theta_1)}{\phi'(\theta_1)}.$$

Now construct the function

$$\xi(u,\alpha) = (u-\alpha_1)(u-\alpha_2) - - (u-\alpha_n).$$

Each of the coefficients of $\xi(u,\alpha)$ is a rational symmetric function of the α's, hence is a number in $\Omega(\theta)$, as has just been shown. $\xi(u,\alpha)$ is a function in $\Omega(\theta)$, and is irreducible in $\Omega(\theta)$,

since any factor in $\Omega(\theta_1)$ would vanish for some α_i, hence for all since the Galois group is transitive, and any permutation replacing α_i by α_j leaves ω_1 unchanged. α_1 is, then, a root of an equation of the r'th degree in $\Omega(\theta)$, and the theorem is proved.

Theorem XV. If θ is a number in a sub-domain $\Omega(\omega)$ of the Galois domain $\Omega(\rho)$, then if θ is represented as

$$\theta = f(\rho) = a_0 + a_1\rho + - - + a_\kappa\rho^\kappa,$$

$f(\rho)$ cannot be of lower degree than $m = \frac{n}{r}$, where r is the order of the domain $\Omega(\omega)$.

Proof:

If ω has r conjugates, there are $m = \frac{n}{r}$ numbers such that

$$\phi(\omega) = \theta = f(\rho) = f(\rho') = - - f(\rho^{(m-1)}),$$

as has been shown in the preceding theorem.

That is,

$$a_0 + a_1\rho + - - - + a_\kappa\rho^\kappa - \theta = 0,$$
$$a_0 + a_1\rho' + - - - + a_\kappa\rho'^\kappa - \theta = 0,$$
$$- \; - \; - \; - \; - \; - \; - \; - \; - \; - \; -$$
$$a_0 + a_1\rho^{(m-1)} + - - - + a_\kappa\rho^{(m-1)\kappa} - \theta = 0.$$

But this system of equations is equivalent to the statement that $\rho, \rho', - - \rho^{(m-1)}$, are all roots of the equation in $\Omega(\omega)$

$$a_0 + a_1x + - - - + a_\kappa x^\kappa - \theta = 0;$$

and this impossible if $k < m$ unless the given equation vanishes identically, which again is impossible if $\theta \neq 0$ and $a_0, a_1, - - a_\kappa$ are rational numbers. Hence $k \geq m$.

Theorem XVI. A necessary and sufficient condition that an equation $F(x) = 0$ be a normal equation is, that its Galois group be transitive and of the same order as the degree of $F(x)$.

A. Assume $F(x) = 0$ a normal equation.

Then by hypothesis all its roots can be expressed in terms of some one of them; suppose that

$$\alpha_2 = f_2(\alpha_1), \quad \alpha_3 = f_3(\alpha_1), \quad - - \quad \alpha_n = f_n(\alpha_1).$$

Now $\alpha_1, \alpha_2, - - \alpha_n,$ are all conjugate, therefore the Galois group is transitive and of an order at least as great as n. Then if the group were of an order greater than n, it would contain some permutation, not the identity, which would leave some α_i unchanged. This is impossible here, since all the roots can be expressed in terms of any one of them. Therefore the order of the Galois group is equal to n.

B. Assume the group transitive and of order n.

Then all the roots of $F(x) = 0$ are conjugate; $F(x)$ is irreducible in $\Omega(1)$, and any one root has a number of conjugates, including itself, equal to the order of the domain. Therefore α_i is a primitive number in $\Omega(\alpha_1, \alpha_2, - - \alpha_n)$, and $F(x) = 0$ is a normal equation.

CHAPTER III. FUNCTIONS BELONGING TO GROUPS.

A function $\varphi = \varphi(\alpha_1, \alpha_2, - - \alpha_n)$ is defined to belong to Q, a sub-group of P, if it is transformed into itself by every permutation of Q, and into something else by every permutation not in Q.

Theorem I. If a function $\varphi_1 = \varphi_1(\alpha_1, \alpha_2, - - \alpha_n)$ belongs to a sub-group Q of the Galois group P, and if

$$P = Q, \quad Q\pi_2, \quad Q\pi_3, \quad - - \quad Q\pi_{n_2}$$

then if $\varphi_2, \varphi_3, - - \varphi_n,$ are the functions into which φ_1 is trans -

formed by π_2, π_3, - - π_n, then ψ_1, ψ_2, - - ψ_n, are roots of an equation in $\Omega(1)$, irreducible, and of the r'th degree.

Proof:

$$\text{Let} \quad Q = 1, \ s_2, \ s_3, \ - - \ s_q.$$

Then by hypothesis

$$\psi_1 = \psi_1 . s_2 = \psi_1 . s_3 = - - = \psi_1 . s_q .$$

Let $\psi_j = \psi_1 . \pi_j$. Then

$$\psi_1 . s_i \pi_j = (\psi_1 . s_i) . \pi_j = \psi_1 . \pi_j = \psi_j .$$

Therefore all the permutations of the co-set $Q\pi_j$ transform ψ_1 into the one function ψ_j.

Since $P \equiv Q, \quad Q\pi_2, \quad - - \quad Q\pi_n,$

then the functions ψ_1, ψ_2, - - ψ_n, and only these result when ψ_1 is operated on by all the permutations of the Galois group.

If
$$\psi_i = \psi_j ,$$
$$\psi_1 . \pi_i = \psi_1 . \pi_j ,$$
$$\psi_1 = \psi_1 . \pi_j \pi_i^{-1} ,$$
and
$$\pi_j \pi_i^{-1} = s_k ;$$
$$\pi_j = s_k \pi_i ,$$

contrary to hypothesis. Therefore these functions are all distinct.

Let
$$\phi(t) = (t-\psi_1)(t-\psi_2) \ - - \ (t-\psi_n).$$

The coefficients of $\phi(t)$ are rational symmetric functions of the ψ's, hence must be transformed into themselves by every permutation of the Galois group. $\phi(t)$ is therefore a function in $\Omega(1)$, and is irreducible since all its roots are conjugate.

Theorem of Lagrange. Every function in the domain $\Omega(\alpha_1, \alpha_2, -\alpha_n)$ which permits the permutations of a sub-group Q of the Galois group P is contained in the domain $\Omega(\psi_1)$, if ψ_1 is a function belonging to Q.

Let ω_1 be a function which permits the permutations of Q, and let ψ_1 belong to Q.

Assume

$$P = Q, \quad Q\pi_2, \quad - - \quad Q\pi_n,$$

and $$\psi_2 = \psi_1 . \pi_2 , \quad \psi_3 = \psi_1 . \pi_3 , \quad - - \quad \psi_n = \psi_1 . \pi_n .$$

Then by the previous theorem $\psi_1, \psi_2, \; - - \; \psi_n$, are all distinct, and

$$\phi(t) = (t-\psi_1)(t-\psi_2) \; - - - \; (t-\psi_n)$$

is a function of t irreducible in $\Omega(1)$.

Suppose $$\omega_2 = \omega_1 . \pi_2 , \quad \omega_3 = \omega_1 . \pi_3 , \quad - - \quad \omega_n = \omega_1 . \pi_n .$$

Then all the conjugates of ω_1 are among these functions, although these functions are not necessarily distinct.

Construct $$\phi(t) \left\{ \frac{\omega_1}{t - \psi_1} + \frac{\omega_2}{t - \psi_2} + - - + \frac{\omega_n}{t - \psi_n} \right\} = \Phi(t)$$

$\Phi(t)$ is a function in $\Omega(1)$, since its coefficients are rational symmetric functions of the roots of the original equation.

Then $$\omega_1 \phi'(\psi_1) = \Phi(\psi_1),$$

$$\omega_1 = \frac{\Phi(\psi_1)}{\phi'(\psi_1)} .$$

This proves the theorem.

Theorem II. Given a function $\psi(\alpha_1, \alpha_2, \; - - \; \alpha_n)$ of the roots of the equation $F(x) = 0$ which belongs to a sub-group Q of the Galois group P, then by the adjunction of ψ to $\Omega(1)$ the group P reduces to Q.

Proof:

Given ψ belonging to Q, then by Lagrange's theorem every function which remains unchanged under the permutations of Q is a number in $\Omega(\psi)$; Q is contained in P, therefore the

permutations of Q leave valid all rational equations in $\Omega(\psi_1)$ between the roots of the equation F(x) = 0. Q therefore satisfies the conditions of being the Galois group with respect to $\Omega(\psi_1)$, by Theorem X, Chapter II.

Theorem III. If Q, Q', - - $Q^{(n)}$ are a set of conjugate sub-groups of P, and R is their cross-cut, then if $\psi_1, \psi_2,$ - - ψ_k, are functions conjugate to ψ_1, which belongs to Q, by the simultaneous adjunction of $\psi_1, \psi_2,$ - - ψ_k, to $\Omega(1)$ the Galois group reduces to R.

Proof:

Let $P = Q, \; Q\pi_2, \; - - \; Q\pi_k,$

and let $\psi_i = \psi_1 . \pi_i$.

Then
$$\psi_i . \pi_i^{-1} = \psi_1,$$
$$\psi_1 . s_j = \psi_1,$$
$$\psi_1 . \pi_i = \psi_i.$$
and
$$\psi_i . \pi_i^{-1} Q \pi_i = \psi_i;$$

therefore ψ_i permits the permutations of $\pi_i^{-1} Q \pi_i$. Also, $\pi_i^{-1} Q \pi_i$ is included in the group K to which ψ_i belongs; if K were of an order larger than the order of Q, there would be fewer co-sets of P with respect to K, and hence ψ_i would have fewer conjugates than ψ_1 has, which is not the case. Therefore $\pi_i^{-1} Q \pi_i$ is the sub-group to which ψ_i belongs.

Now let
$$\omega_1 = a\psi_1 + b\psi_2 + - - - + m\psi_k ;$$
a, b, - - m can be so chosen, rationally, that all the ω's will be distinct when the ψ_i's are permuted among themselves in every possible way. Then ω_i is unchanged by all the permutations of R, the cross-cut of the sub-groups conjugate to Q, and only by these;

for if any permutation leaves ω_1 unchanged it must transform ψ_1, ψ_2, - - ψ_k each into itself, and is therefore a permutation common to all the conjugates of Q. Therefore ω_1 is a function belonging to R, and by Theorem II the Galois group is reduced to R by the adjunction of ω to $\Omega(1)$.

Theorem IV. A necessary and sufficient condition that exactly k of the conjugates ψ_1, ψ_2, - - ψ_m, be expressible rationally in terms of any one of them ψ_1, is that the sub-group Q to which ψ_1 belongs be of index k under the sub-group K of P which transforms Q into itself.

For, if Q is of index k under K, then with the terminology of the preceding theorem

$$Q = \pi_2^{-1} Q \pi_2 = \pi_3^{-1} Q \pi_3 = - - = \pi_k^{-1} Q \pi_k,$$

for some set of k π_i's.

Hence ψ_2, ψ_3, - - ψ_k, have the same group Q, and by Lagrange's theorem each of the functions ψ_1, ψ_2, - - ψ_k, which permit the permutations of Q, can be expressed rationally in terms of ψ_1.

Also, if

$$\psi_2 = \phi_2(\psi_1), \quad \psi_3 = \phi_3(\psi_1), \quad - - \quad \psi_k = \phi_k(\psi_1),$$

where ϕ_2, ϕ_3, - - ϕ_k, are functions in $\Omega(1)$, then since each of these equations is left valid by all permutations of the Galois group, if Q leaves ψ_1 unchanged it must leave ψ_2, ψ_3, - - ψ_k, unchanged. ψ_1, ψ_2, - - ψ_k, are all conjugate, therefore the group Q is of the same order as the groups to which ψ_2, ψ_3, - - ψ_k, belong, and therefore Q must be identical with these groups.

Therefore

$$Q = \pi_2^{-1} Q \pi_2 = \pi_3^{-1} Q \pi_3 - - = \pi_k^{-1} Q \pi_k.$$

Now if π_i, π_j transform Q into itself, $\pi_i \pi_j$ must also

transform Q into itself. The operations of the sets Q, $Q\pi_2$, - - $Q\pi_k$, when combined in every possible manner, form a sub-group of P, of which Q is an invariant sub-group. If this group K were of order $lq > kq$, then $l > k$, and by the first part of the proof there would be more than k conjugates ψ_i, any one of which could be expressed in terms of any other one. This is contrary to hypothesis, and there are at least kq permutations of P which transform Q into itself, since the co-sets $Q\pi_i$ have no operations in common. This proves the theorem.

Now if Q' is some sub-group conjugate to Q, but not identical with it, then if ψ_l is one of the m functions belonging to Q', ψ_l must be distinct from the functions already considered, since $Q' \neq Q$. Then Q' is also invariant and of index k under a group K'*, hence ψ_l has k conjugates any one of which can be expressed in terms of any other. Continuing in this way, it is seen that the m conjugates ψ_i may be divided into sets

$$\begin{array}{llcl} \psi_1, & \psi_2, & - - & \psi_k, \\ \psi_{k+1}, & \psi_{k+2}, & - - & \psi_{2k}, \\ - & - & - - & - \\ \psi_{nk+1}, & \psi_{nk+2} & - - & \psi_m, \end{array}$$

such that every ψ in one set may be expressed rationally in terms of any other in the same set.

Theorem V. If ψ_1 is a function belonging to Q, and if $\psi_2, \psi_3,$ - - ψ_m, are the conjugates of ψ_1, then if R is the cross-cut of the groups Q', Q", - - conjugate to Q, and

$$\phi(t) = (t-\psi_1)(t-\psi_2) \quad - - \quad (t-\psi_m),$$

the Galois group of $\phi(t)$ is simply isomorphic with P/R.

Burnside, Theory of Groups, 2d Edition, page 32.

Lemma: The permutations of $R\pi_i$ and only these permute ψ_1, ψ_2, - - ψ_m, in a given way, if $R = s_1, s_2, \cdots s_h$, and

$$P = R, \quad R\pi_2, \quad - - - \quad R\pi_n.$$

For R, being common to the sub-groups which leave ψ_1, ψ_2, - - ψ_m respectively, unchanged, must transform each of these functions into itself; and therefore $s_i\pi_j$ $(i = 1, 2, \cdots h)$ must transform the sequence

$$\psi_1, \ \psi_2, \quad - - \ \psi_m,$$

in the same way. Now if π_i, π_j, transform this sequence in the same way, $\pi_j \pi_i^{-1}$ must transform the sequence into itself.

Then $$\pi_j \pi_i^{-1} = s_K,$$

and $$\pi_j = s_K \pi_i^{-1}.$$

Therefore the co-sets R, $R\pi_2$, - - $R\pi_n$ must each transform the given sequence in a different way.

Let $$\omega_1 = a_1\psi_1 + a_2\psi_2 + - - + a_m\psi_m$$

where a_1, a_2, - - a_m are rational numbers so chosen that ω_1 is transformed into something else whenever permutations of P interchange the ψ_i's among themselves.

Now if ω_2, ω_3, - - ω_K, are the conjugates of ω_1, these all belong to the same sub-group R, therefore by Lagrange's theorem any one of them can be expressed rationally in terms of any other one. Then

$$\phi(t) = (t-\omega_1)(t-\omega_2) \ - - \ (t-\omega_K) = 0$$

is an equation in $\Omega(1)$, since its coefficients are left unchanged by every permutation of the Galois group P; it is irreducible, since its roots are all conjugate and distinct. By the above discussion it is also a normal equation.

The domain $\Omega(\omega_1)$ is, then, a normal domain, and by Theorem VI, Chapter II, the substitutions (ω_1, ω_2) form the Galois group

of the domain.

Let $\omega_2 = f_2(\omega_1)$, $\omega_3 = f_3(\omega_1)$, - - - $\omega_k = f_k(\omega_1)$.

If ω_1 is operated on by the co-sets $R\pi_i$, (i=1, 2, - - k), the same set of ω's will result in each case, in some order.

Suppose $\omega_i = \omega_1 . \pi_i$,

and assume $(\omega_1, \omega_i) \sim \pi_i$.

Then

ω_1, $f_2(\omega_1)$, - - - $f_k(\omega_1)$

operated on by the substitution (ω_1, ω_i) gives

(1) ω_i, $f_2(\omega_i)$, - - - $f_k(\omega_i)$

(2) $= \omega_1 . \pi_i$, $f_2(\omega_1 . \pi_i)$ - - - $f_k(\omega_1 . \pi_i)$

(3) $= \omega_1 . \pi_i$, $f(\omega_1) . \pi_i$ - - - - $f_k(\omega_1) . \pi_i$

(4) $= f_i(\omega_1)$, $f_2'(\omega_1)$, - - - - $f_k'(\omega_1)$.

Now if this sequence is operated on by (ω_1, ω_j), it becomes

(5) $f_i(\omega_j)$, $f_2'(\omega_j)$, - - - - $f_k'(\omega_j)$

(6) $= f_i(\omega_1 . \pi_j)$, $f_2'(\omega_1 . \pi_j)$, - - - $f_k'(\omega_1 . \pi_j)$

(7) $= f_i(\omega_1) . \pi_j$, $f_2'(\omega_1) . \pi_j$, - - - $f_k'(\omega_1) . \pi_j$.

From the identity of (1),(2),(3), and (4), it follows that (5) is identical with

(8) $\omega_1 . \pi_i \pi_j$, $f_2(\omega_1) . \pi_i \pi_j$, - - - $f_k(\omega_1) . \pi_i \pi_j$.

Now it was assumed that π_i corresponded to (ω_1, ω_i), π_j to (ω_1, ω_j); from (8) it follows that $(\omega_1, \omega_i)(\omega_1, \omega_j)$ corresponds to $\pi_i \pi_j$, since it gives the same result. Therefore the group whose operators are $R\pi_i$ is simply isomorphic with the group of substitutions (ω_1, ω_i), which is the Galois group of the domain $(\Psi_1, \Psi_2, - - \Psi_m)$.

If $\Omega(\alpha_1, \alpha_2, - - \alpha_n)$ is the Galois domain of the equation

F(x) = 0, whose roots are $\alpha_1, \alpha_2, - - \alpha_n$, then any function in $\Omega(\alpha_1, \alpha_2, - - \alpha_n)$ is called a *natural irrationality*.

Theorem VI. Every possible reduction of the Galois group is obtained by the adjunction of a natural irrationality. If the index of the reduced group under the original one is j, the reduction cannot be accomplished by the adjunction of a domain of an order less than j. Its order may be equal to j, in which case the adjoined irrationality is a natural one. If the order of the adjoined domain is greater than j it is a multiple of j.

Given F(x), and g(t) its Galois resolvent. If g(t) is to be reducible in a domain Ω' over $\Omega(1)$, there is an algebraic number ε, such that

$$\Omega(\varepsilon) = \Omega'.$$

By hypothesis g(t) has a factor $g_1(t)$, in $\Omega(\varepsilon)$.

If q is the degree of $g_1(t) = g_1(t, \varepsilon)$, let

$$\rho_1, \rho_2, - - \rho_q,$$

be its roots.

$$g_1(t, \varepsilon) = (t-\rho_1)(t-\rho_2) - - (t-\rho_q).$$

Then the substitutions (ρ_1, ρ_i), (i=1, 2, - - q) form a group.

For, let $$\rho_i = \theta(\rho_1).$$

Then $g_1[\theta_i(t)\varepsilon]$ has one root, $t=\rho_1$, in common with $g_1(t)=0$. $g_1(t)$ was assumed irreducible in $\Omega(\varepsilon)$; hence if the two functions have a common factor, this common factor can be found by rational processes, hence is also a function in $\Omega(\varepsilon)$. The factor must therefore be $g_1(t, \varepsilon)$ itself. Then $g_1[\theta_i(t), \varepsilon]$ is divisible by $g_1(t, \varepsilon)$, and must vanish for all its roots $\rho_1, \rho_2, - - \rho_q$.

Hence $\theta_i(\rho_j) = \rho_k$, one of the roots of $g_1(t, \varepsilon)$.

From this result it follows that $(\rho_1, \rho_j) = (\rho_i, \rho_k)$,

$$(\rho_1, \rho_i)(\rho_1, \rho_j) = (\rho_1, \rho_i)(\rho_i, \rho_k)$$
$$= (\rho_1, \rho_k),$$

another substitution of the set. Since any ρ_i can be taken as the one in terms of which the rest are to be expressed, it follows that if (ρ_1, ρ_i) is in the set, (ρ_i, ρ_1) is also in the set. These substitutions must therefore form a group.

Let this group be Q, necessarily a sub-group of P, and suppose it of index j under P.

Then $g_1(t,\varepsilon)$ permits all the permutations of Q; if ψ_1 is a function belonging to Q, then by Lagrange's theorem the coefficients of $g_1(t,\varepsilon)$ can be expressed rationally in terms of ψ_1.

Consequently $g_1(t,\varepsilon)$ can be written $G(t,\psi_1)$.

Since Q is of index j, ψ_1 has j conjugates, and ψ_1 is a root of an equation in $\Omega(1)$ of degree j.

Let this equation be

$$\phi(u) = (u-\psi_1)(u-\psi_2) \quad - \quad - \quad (u-\psi_j) = 0.$$

Now $G(t,\psi_1)$ vanishes for $t= \rho_1, \rho_2,$ - - ρ_q; hence it must also vanish when operated on by all the permutations of the Galois group P. Hence there result the j factors

$$G(t,\psi_1), \quad G(t,\psi_2), \quad - \quad - \quad G(t,\psi_j).$$

These can have no factors in common, for in that case their product, g(t), would be reducible in $\Omega(1)$.

Suppose t chosen rationally so that

$$G(t,\psi_i) \neq G(t,\psi_1),$$

and therefore $$G(t,\psi_i) \neq g_1(t,\varepsilon), \qquad (i= 2, - - j)$$

while $$g_1(t,\varepsilon) = G(t,\psi_1).$$

Therefore

$$G(t,u) - g_1(t,\varepsilon), \qquad \phi(u)$$

have only one factor $u - \psi_1$, in common.

Then

$$F(u)\left\{G(t,u) - g_1(t,\varepsilon)\right\} + \Phi(u)\phi(u) = u - \psi_1;$$

if $u = k$, another rational number,

$$F(k,\varepsilon) = k - \psi_1,$$

and ψ_1 can be expressed rationally as a function of ε . Therefore ψ_1 is contained in $\Omega(\varepsilon)$, and the order of $\Omega(\varepsilon)$ is some multiple of the order of $\Omega(\psi_1)$.

It has been shown that the coefficients of $g_1(t)$ can be expressed as rational functions of a natural irrationality. If the order of $\Omega(\varepsilon)$ is the same as that of $\Omega(\psi_1)$, ψ_1 is a primitive number in $\Omega(\varepsilon)$, and ε can be expressed rationally in terms of ψ_1. In that case ε is a natural irrationality.

3

CHAPTER IV. A GENERAL SOLUTION OF THE QUARTIC.

Assume the general equation of the fourth degree written in the form

$$x^4 + a_1 x^3 + a_2 x^2 + a_3 x + a_4 = 0,$$

where a_1, a_2, a_3, a_4 are rational numbers not all zero.

Let

$$\rho = (\alpha_1 - \alpha_2)^2 + a(\alpha_2 - \alpha_3)^2,$$

and let $\rho_2, \rho_3, \cdot - - \rho_K$, be the functions resulting when α_1, α_2, α_3, α_4, are permuted in every possible way.

Now the group leaving $(\alpha_1 - \alpha_2)^2$ unchanged is,

$$1, \quad 12, \quad 34, \quad 12\cdot 34\ ;$$

that leaving $(\alpha_2 - \alpha_3)^2$ unchanged is,

$$1, \quad 14, \quad 23, \quad 14\cdot 23\ .$$

These two groups have only the identity in common, and therefore ρ is left unchanged in form only by the identity. Now if the squares of all possible differences of the ρ's, $(\rho_i - \rho_j)$ $i \neq j$, are formed and multiplied together, there results a rational integral function containing a, since this will be a rational symmetric function of the α's. When equated to zero, this equation which results can have only a finite number of roots. a can be chosen in an infinite number of ways so that it does not satisfy this equation, and when a is so chosen ρ has 24 distinct values. It is therefore a primitive number in $\Omega(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$.

If

$$g(t) = (t-\rho_1)(t-\rho_2) - - (t-\rho_{24}),$$

g(t) is the Galois resolvent of the given quartic, and the quartic will have been solved when ρ has been expressed in terms of known quantities.

The functions $(\alpha_1 - \alpha_2)^2$, $(\alpha_2 - \alpha_3)^2$ are roots of the equation of squared differences,

$$\phi(t) = \left[t-(\alpha_1-\alpha_2)^2\right]\left[t-(\alpha_1-\alpha_3)^2\right]\left[t-(\alpha_1-\alpha_4)^2\right]\left[t-(\alpha_2-\alpha_3)^2\right]\left[t-(\alpha_2-\alpha_4)^2\right]\left[t-(\alpha_3-\alpha_4)\right] .$$

$\phi(t)$ can be solved indirectly in the following manner.

Let
$$X_1 = (\alpha_1 - \alpha_2)^2 + (\alpha_3 - \alpha_4)^2,$$
$$X_2 = (\alpha_1 - \alpha_3)^2 + (\alpha_2 - \alpha_4)^2,$$
$$X_3 = (\alpha_1 - \alpha_4)^2 + (\alpha_2 - \alpha_3)^2,$$

and
$$Y_1^2 = (\alpha_1 - \alpha_2)^2(\alpha_3 - \alpha_4)^2,$$
$$Y_2^2 = (\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_4)^2,$$
$$Y_3^2 = (\alpha_1 - \alpha_4)^2(\alpha_2 - \alpha_3)^2.$$

Also, let
$$Z_1 = (\alpha_1 - \alpha_2)^2 - (\alpha_3 - \alpha_4)^2,$$
$$Z_2 = (\alpha_1 - \alpha_3)^2 - (\alpha_2 - \alpha_4)^2,$$
$$Z_3 = (\alpha_1 - \alpha_4)^2 - (\alpha_2 - \alpha_3)^2.$$

Then
$$X_1^2 = (\alpha_1 - \alpha_2)^4 + (\alpha_3 - \alpha_4)^4 + 2(\alpha_1 - \alpha_2)^2(\alpha_3 - \alpha_4)^2,$$
$$Z_1^2 = (\alpha_1 - \alpha_2)^4 + (\alpha_3 - \alpha_4)^4 - 2(\alpha_1 - \alpha_2)^2(\alpha_3 - \alpha_4)^2.$$

Therefore
$$Z_1^2 = X_1^2 - 4Y_1^2 ,$$
$$Z_2^2 = X_2^2 - 4Y_2^2 ,$$
$$Z_3^2 = X_3^2 - 4Y_3^2 ,$$

and
$$Z_1 = \pm\sqrt{X_1^2 - 4Y_1^2}$$
$$Z_2 = \pm\sqrt{X_2^2 - 4Y_2^2}$$
$$Z_3 = \pm\sqrt{X_3^2 - 4Y_3^2} .$$

Now
$$(\alpha_1 - \alpha_2)^2 = 1/2(X_1 + Z_1),$$
$$(\alpha_3 - \alpha_4)^2 = 1/2(X_1 - Z_1),$$

and similarly for the other functions.

Let

$$a = (\alpha_1 - \alpha_2)^2, \qquad a' = (\alpha_3 - \alpha_4)^2,$$
$$b = (\alpha_1 - \alpha_3)^2, \qquad b' = (\alpha_2 - \alpha_4)^2,$$
$$c = (\alpha_1 - \alpha_4)^2, \qquad c' = (\alpha_2 - \alpha_3)^2.$$

Then

$$a = 1/2(X_1 + \sqrt{X_1^2 - 4Y_1^2}), \qquad a' = 1/2(X_1 - \sqrt{X_1^2 - 4Y_1^2}),$$
$$b = 1/2(X_2 + \sqrt{X_2^2 - 4Y_2^2}), \qquad b' = 1/2(X_2 - \sqrt{X_2^2 - 4Y_2^2}),$$
$$c = 1/2(X_3 + \sqrt{X_3^2 - 4Y_3^2}), \qquad c' = 1/2(X_3 - \sqrt{X_3^2 - 4Y_3^2}).$$

From these equations the roots of the equation of squared differences can be found when the auxilliary functions X_1 and Y_1^2 are known.

Now

$$X_1 = (\alpha_1 - \alpha_2)^2 + (\alpha_3 - \alpha_4)^2,$$
$$Y_1^2 = (\alpha_1 - \alpha_2)^2(\alpha_3 - \alpha_4)^2.$$

X_1 belongs to the group

1, 12 34, 12, 34, 1324, 1423,

and evidently Y_1^2 belongs to the same group.

Let $$X(t) = (t - X_1)(t - X_2)(t - X_3).$$

The coefficients of $X(t)$ are rational symmetric functions of the roots $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ hence can be expressed rationally in terms of the coefficients of the quartic. These coefficients, expressed as functions of the sums of like powers of the roots,* are as follows.

$$-B_1 = X_1 + X_2 + X_3 = 3s_2 - 2a_2 .$$
$$B_2 = X_1X_2 + X_1X_3 + X_2X_3 = 3s_1^2 - 4s_1s_3 + 4s_4.$$
$$-B_3 = X_1X_2X_3 = 2s_2^3 + 2s_3^2 - 3s_2s_4 - 2s_1s_2s_3 + 4a_2a_4$$
$$+ 4a_2s_4 - 4s_1s_5 - 8a_4s_2 + 6s_6 .$$

$X(t)$ is a cubic with rational coefficients, hence can be solved.

Cajori, Theory of equations: Art. 68.

Now $$X(t)\left\{\frac{Y_1^2}{t-X_1}+\frac{Y_2^2}{t-X_2}+\frac{Y_3^2}{t-X_3}\right\} = \Phi(t)$$

is also a function with rational coefficients, since these are rational symmetric functions of the roots of the quartic.

Then
$$X'(X_1)\,Y_1^2 = \Phi(X_1),$$
$$Y_1^2 = \frac{\Phi(X_1)}{X'(X_1)}$$

Therefore Y_1^2 can be expressed rationally in terms of X_1.

Let $\Phi(t) = At^2 + Bt + C.$

By computation

$$A = a_1^2 + 12a_4 - 6a_1a_3 - a_1^4 + 4a_1^2a_2 + 2s_2^2.$$

$$-B = 6s_6 - 3s_2s_4 - 4s_1s_5 + 2s_2^3 + 2s_3^2 + 4a_2s_4 - 8a_4s_2$$
$$- 2s_1s_2s_3 + 4a_2a_4.$$

$$C = 2s_1s_3s_4 + s_2^2s_4 - s_2s_6 - s_4^2 - 2s_3s_5 - 2s_2s_3^2 - s_1^2s_6$$
$$+ a_4\left(8s_1^2s_2 - 12s_2^2 - 26s_1s_3 + 42s_4 - 72a_4\right).$$

By means of $X'(t)$ and $\Phi(t)$, then, Y_1^2, Y_2^2, Y_3^2, can be expressed as functions of X_1, X_2, X_3, respectively; then by the aid of the equations on page 38 the required roots of the equation of squared differences can be found. This completes the theoretical reduction of the Galois resolvent; the actual determination of the roots α_1, α_2, α_3, α_4, can, however, be carried out more easily as follows.

Given a, b, c, a', b', c', then

$$a + b + c = 3\alpha_1^2 - 2(\alpha_2 + \alpha_3 + \alpha_4) + \alpha_2^2 + \alpha_3^2 + \alpha_4^2$$
$$= 4\alpha_1^2 - 2(\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4)\,\alpha_1 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2 + \alpha_4^2$$
$$= 4\alpha_1^2 - 2s_1\alpha_1 + s_2.$$

This is an equation of the second degree which α_1 must satisfy.

$$\text{Given} \quad a = (\alpha_1 - \alpha_2)^2 \qquad a' = (\alpha_3 - \alpha_4)^2$$
$$b = (\alpha_1 - \alpha_3)^2 \qquad b' = (\alpha_2 - \alpha_4)^2$$
$$c = (\alpha_1 - \alpha_4)^2 \qquad c' = (\alpha_2 - \alpha_3)^2.$$

$$\begin{aligned}\text{Then} \quad a' + b' + c' &= 2\alpha_2^2 + 2\alpha_3^2 + 2\alpha_4^2 - 2(\alpha_3\alpha_4 + \alpha_2\alpha_4 + \alpha_2\alpha_3) \\ &= 2(\alpha_1^2 + \alpha_2^2 + \alpha_3^2 + \alpha_4^2) - 2\sum \alpha_1\alpha_2 \\ &\quad + 2(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_1\alpha_4 + \alpha_1^2) - 4\alpha_1^2 \\ &= 2s_2 - 2a_2 + 2s_1\alpha_1 - 4\alpha_1^2,\end{aligned}$$

another equation which α_1 must satisfy. The two are identical, however; for

$$\begin{aligned}a' + b' + c' &= X_1 + X_2 + X_3 - (a + b + c) \\ &= 3s_2 - 2a_2 - (a + b + c) \\ &= 3s_2 - 2a_2 - (4\alpha_1^2 - 2s_1\alpha_1 + s_2) \\ &= 2s_2 - 2a_2 + 2s_1\alpha_1 - 4\alpha_1^2,\end{aligned}$$

which is identical with the second equation above.

Therefore the value of α_1 found by adding together a', b', c' is the same as that found by adding together the elements of the first column and solving the quadratic for α_1.

Now in the actual solution of the quartic by this method, there is no way of distinguishing between the functions a, b, c, and a', b', c'; all that is given is 6 functions, divided up into sets of two. The sum of three of these, one being chosen from each set, is equal to a quantity N such that

$$\text{either} \qquad 4\alpha_1^2 - 2s_1\alpha_1 + s_2 = N,$$

$$\text{or} \qquad -4\alpha_1^2 + 2s_2\alpha_1 - 2a_2 + 2s_2 = N.$$

Each equation has two roots, and one of these four roots must be α_1. The particular value of α_1 can be found by substituting these four roots in the quartic, and choosing the one which satisfies it.

The other three roots can be foun' by combining a with b, c, b', c' in the three other possible ways, and proceeding as above. As has been shown, the combination of a' with the functions b, c, b', c', would give the same results as would already have been obtained by combining them with a.